European Journal of Sustainable Development (2025), **14**, 2, 643-660 ISSN: 2239-5938
Doi: 10.14207/ejsd.2025.v14n2p643

Hybrid Warfare and Customs Security: Strengthening Resilience for Sustainable Development

By Irina Lomachinska[1], Mykhailo Ishchuk[2], Ivan Chornomordenko[3], Ganna Taran[4], Maryna Turchyn[5], Natalia Martsinko[6], Kateryna Pasko[7], Olena Lobanchuk[8]

ABSTRACT:
This article examines the threats facing Ukraine's customs system in the context of hybrid warfare waged by the Russian Federation in the digital era. It explores key scientific approaches to defining the concept of "hybrid warfare", which is characterized as a complex, multidimensional phenomenon that integrates military, informational, cyber, economic, and political instruments of influence. This form of aggression complicates the identification, counteraction, and neutralization processes, while simultaneously posing a threat to critical components of national resilience. The article emphasizes that hybrid warfare targets the disruption of essential infrastructure, including law enforcement agencies, healthcare systems, food security, transportation networks, the economy, and other sectors vital to the functioning of the state. Particular attention is given to the indirect influence tools employed by the aggressor state, such as support for separatist and terrorist groups, which may involve financing, arming, and carrying out acts of state terrorism. The article also highlights the impact of informational and psychological campaigns designed to transform public opinion destructively in the targeted countries. In the case of Ukraine's customs service, it outlines the diverse methods of hybrid influence, including economic pressure through customs mechanisms, the creation of artificial trade barriers, the spread of contraband, cyberattacks on customs infrastructure, campaigns to discredit customs authorities, the use of corruption schemes, and political-legal manipulations aimed at delaying reforms and influencing foreign economic agreements. The article concludes that customs security has become a priority not only for national security but also as an essential element in achieving the United Nations' Sustainable Development Goals related to peace, justice, institutional resilience, and economic stability. The article underscores the need for the digital transformation of Ukraine's customs system as a strategic response to modern challenges. Such transformation will help strengthen institutional resilience, enhance public trust, ensure procedural transparency, and improve Ukraine's position in the global information space.

Keywords: hybrid warfare, customs security, digital transformation, cyber threats, institutional resilience, information security, sustainable development goals, economic stability

[1]Doctor of Philosophy (Hb.), Professor, Department of Philosophy and Religious Studies, Borys Grinchenko Kyiv Metropolitan University, https://orcid.org/0000-0003-2537-6322
[2] Senior Lecturer at the Department of Customs Affairs and Commodity Science, State Tax University, Irpin, Ukraine. https://orcid.org/0000-0001-9346-2607 (Corresponding Author)
[3]Doctor of Philosophy (Hb.), Professor, Department of Philosophy, Kyiv National University of Construction and Architecture, Kyiv, Ukraine, https://orcid.org/0000-0002-9204-6342
[4]PhD, Senior Lecturer, Department of Philosophy, Kyiv National University of Construction and Architecture, Kyiv, Ukraine, https://orcid.org/0000-0003-3311-0321
[5]PhD, Senior Lecturer, Department of Philosophy, Kyiv National University of Construction and Architecture, Kyiv, Ukraine, https://orcid.org/0000-0001-8506-4027
[6]Senior Research Fellow, Army Science Center of the Hetman Petro Sahaydachnyi National Army Academy, Lviv, Ukraine, https://orcid.org/0000-0001-9267-6136
[7]PhD, Associate Professor, Department of Psychology, Sumy State Pedagogical University named after A. S. Makarenko, Sumy, Ukraine, https://orcid.org/0000-0003-0488-9719
[8]PhD, Associate Professor, Department of Ethics and Esthetics, Dragomanov Ukrainian State University, https://orcid.org/0000-0002-1466-0398

1. Introduction

In the current context of evolving international relations and a globalized economy, hybrid wars have become one of the key threats to both national and international security. This issue is particularly significant in the context of the armed aggression of the Russian Federation against Ukraine, which has been accompanied by the active use of hybrid instruments of influence. These instruments include not only conventional military operations but also economic pressure, trade restrictions, information and media attacks, as well as cyberattacks and manipulations within the digital environment.

Hybrid aggression is multidimensional in nature and significantly complicates the functioning of the customs security system, rendering it vulnerable to external interference. Such interference includes the illicit movement of goods, smuggling, disruption of logistics chains, the circulation of sanctioned goods, and the broader destabilizing impact on economic indicators. Under conditions of information warfare and digital threats, the issue of ensuring the resilience of customs infrastructure against external intrusions – particularly cyber risks capable of paralyzing or distorting the operation of customs control and monitoring systems – becomes especially critical.

In this regard, customs security should be viewed not only as an element of national security but also as a factor in achieving sustainable development goals, particularly those related to peace, justice, institutional resilience, and economic stability. Effective counteraction to hybrid threats in the customs sphere requires integrated approaches encompassing legal, technological, economic, and organizational dimensions.

The study of this complex set of challenges is highly relevant in the context of Ukraine's evolving security policy and its aspirations for European integration. In this context, particular attention should be paid to the process of aligning Ukraine's customs legislation and institutional practices with the standards of the European Union. Ukraine has already fulfilled nearly 80 percent of its obligations regarding the implementation of the provisions of the Union Customs Code, reflecting substantial progress in the legal harmonization and functional modernization of its customs system. These developments contribute to strengthening institutional resilience and enhancing the capacity of customs authorities to respond effectively to hybrid threats.

2. Theoretical Background

The complexity and multifaceted character of the research problem necessitated an interdisciplinary approach and a diverse source base. Central to this inquiry are academic contributions that examine the nature of hybrid warfare and the principal strategies through which it is executed in today's globalized environment. Particularly relevant are studies that engage with the multidimensional discourse on hybrid warfare from the standpoint of key Western actors – including NATO, the United States, and the European Union. Scholars assess the hybrid capabilities of Russia and China, highlight the growing threat of cyber warfare, and present global case studies that illustrate the implementation of hybrid tactics, offering practical insights into forms of resistance (Mumford, 2018).

Khorram-Manesh and Burkle (2022) conduct a systematic review of humanitarian and health-related consequences of hybrid warfare, emphasizing the specific challenges it poses to civilian populations and the need to adapt humanitarian and medical response frameworks accordingly. Their inquiry is further developed in a subsequent publication (Khorram-Manesh et al., 2023), which focuses specifically on the social and healthcare repercussions of the Russian-led hybrid war in Ukraine, contributing to a more nuanced understanding of its impact on civilians.

The conceptual contours of hybrid warfare as a novel form of international armed conflict are explored by Glukh and Honcharenko (2024), who analyze its definitional parameters, strategic implications, and the legal complexities it presents within the evolving field of international law. Their work highlights the need to re-examine the regulatory frameworks that underpin conflict categorization and governance in the context of hybrid threats.

Theoretical considerations regarding the nature, content, and mechanisms of hybrid warfare are further developed by Derevyanko (2023) and Buriachenko (2024), both of whom emphasize the asymmetrical structure of hybrid conflict. Their analyses point to the deliberate fusion of military and non-military instruments, notably cyber operations and disinformation campaigns, which are central to this mode of warfare.

The impact of hybrid warfare on strategic thinking within NATO is the subject of inquiry in the study by Caliskan and Liégeois (2020). Drawing on interviews with NATO officials, the authors contend that the conceptual ambiguity surrounding hybrid warfare may hinder effective strategic planning, underscoring the imperative for conceptual clarity and terminological precision within NATO's doctrinal framework.

A range of studies investigate Russia's application of hybrid warfare strategies in the international arena, particularly in relation to Ukraine. Manolea (2021) characterizes these strategies as asymmetrical and driven by nationalist interests, illustrating how they operate through a combination of political manipulation and targeted influence campaigns. In their analysis of "anxiety geopolitics", Eberle and Daniel (2022), examine how the discourse of hybrid warfare, particularly in the Czech context, intersects with civilizational geopolitics and contributes to a broader sense of ontological insecurity. The narrative of East-West confrontation, in which Russia is cast as the primary adversary, is shown to intensify societal anxieties and inform policy responses grounded in traditional geopolitical dichotomies.

The threat posed by hybrid warfare to national sovereignty is addressed by Radchenko and Chmyr (2022), who argue that information security – encompassing political, socio-economic, military, and cultural domains – is essential for maintaining societal resilience. They call for the development of integrated security systems to mitigate the destabilizing effects of hybrid aggression.

The role of mass media in advancing hybrid aggression is examined by Savliuk (2024), who outlines how Russian television channels and media outlets have long operated in Ukraine to disseminate pro-Kremlin narratives. These activities have since been amplified by coordinated bot farms and information operations designed to provoke domestic unrest and erode public trust in governmental institutions.

From an economic perspective, Bluszcz and Valente (2022) analyze the impact of Russia's hybrid war in the Donbas region, demonstrating the substantial economic damage inflicted upon Ukraine. Their findings underscore the broader socio-economic implications of hybrid conflict and the need for robust response and recovery strategies.

Further insights into the psychological and informational dimensions of hybrid warfare are offered by S. Derevianko (2024), who focuses on the war's psychological and informational effects on both Ukrainian citizens and the international community. In this context, the protection of constitutional rights to information and the mechanisms for ensuring access to reliable information are framed as critical to national resilience.

Steingartner and Galinec (2021) address the increasingly central role of cyber threats and deception in hybrid warfare, arguing that cyber deception holds considerable strategic potential as both a defensive and offensive measure capable of neutralizing adversarial activities and shaping opponent behavior.

A significant cluster of literature addresses the digital transformation of Ukraine's customs infrastructure as a mechanism for countering hybrid threats. Of note is the work of Matsedonska, Kovalenko, and Shtefan (2021), which evaluates best international practices in customs innovation (including electronic declarations, remote clearance technologies, blockchain, and non-intrusive inspection tools) aimed at increasing efficiency and responsiveness. Complementing this, Mykuliak and Stefanyshyn (2019) analyze the legal and operational dimensions of digital communication systems within Ukraine's customs sector, highlighting the critical role of information technologies in strengthening institutional capacity and security.

While these studies offer a valuable overview of international best practices, a comparative assessment of their practical implementation in Ukraine reveals a more complex picture. Survey data analyzed by Bilovodska and Khurdei (2024) show strong business support for digital customs reforms: 85% of companies expressed interest in completing customs clearance before goods physically enter Ukraine, and 75% favored the option of filing declarations from the company's location, irrespective of the goods' whereabouts. More than 80% identified customs formalities – especially document requests, inspections, and sampling – as primary causes of delay. While 60% reported no issues with excessive inspections, the time required for customs clearance remains inconsistent. According to the Guidelines for Customs Policy in Ukraine (2020), straightforward cases average three hours, but more complex scenarios can take up to 336 hours. In contrast, EU countries complete 63% of clearances in under five minutes, with only 9% taking over an hour. This disparity underscores the importance of further automation and risk-based controls. Although blockchain tools have been piloted in Ukraine, full-scale deployment remains limited. Consequently, while digital instruments have shown potential to reduce human involvement and improve transparency, their overall impact on corruption and procedural delays is constrained by uneven implementation. Ukraine's commitments under the EU Association Agreement (including risk analysis, post-clearance audits, and company inspections) remain aspirational in many operational contexts.

So, as hybrid warfare continues to evolve and expand in scope, the intersection between hybrid aggression and customs security emerges as a vital area of inquiry. Understanding this nexus is indispensable for crafting effective defense strategies and safeguarding sustainable national development.

3. Methods

The methodological framework of this study is grounded in a systemic, interdisciplinary, comparative, and analytical approach. This combination enables a comprehensive examination of the phenomenon of hybrid warfare, its impact on the functioning of the customs system, and the challenges it poses to achieving sustainable development goals in the context of security instability.

A range of scientific research methods was employed throughout the study. The method of systemic analysis was used to examine hybrid warfare as a complex and integrated phenomenon that encompasses military, political, economic, informational, and cultural tools. The case study method was applied to conduct an in-depth analysis of specific instances of hybrid warfare, most notably the war initiated by the Russian Federation against Ukraine since 2014. Comparative analysis was used to juxtapose different approaches to countering hybrid threats, thereby allowing for the formulation of potential adaptive models suitable for the Ukrainian context. Content analysis facilitated the examination of strategies of informational influence disseminated through mass media, social networks, and official narratives of the aggressor state (Russia).

The institutional approach was employed to analyze the customs system as a component of public administration operating under crisis conditions. This allowed for the identification of vulnerabilities in existing mechanisms for responding to hybrid threats. The integration of these methodological approaches enables a multidimensional understanding of hybrid warfare, revealing its internal logic, mechanisms of influence, and implications for both national and international security within the broader context of globalization.

Among the empirical methods, a survey was conducted in March–April 2025. Participants included students specializing in law and humanities at Borys Grinchenko Kyiv Metropolitan University and the National University of Construction and Architecture (Kyiv, Ukraine); students enrolled in the "Customs Management" and "Commodity Science and Customs Expertise" programs at the State Tax University (Irpin, Ukraine); and cadets of Hetman Petro Sahaydachnyi National Army Academy (Lviv, Ukraine). In total, the sample comprised 215 students from the first to the fifth year of study, representing youth from across all regions of Ukraine. The average age of the respondents was 22 years. All participants were informed about the purpose of the study and the anonymity of their responses and voluntarily agreed to participate in the survey.

The diagnostic stage relied on a written questionnaire completed via Google Forms, with original content design. Both quantitative and qualitative analytical methods were used to process the collected data. The diagnostic findings were interpreted and synthesized during the final stage of the research.

4. Discussion and Results

Hybrid warfare, as a global threat of the modern era, combines military, informational, cyber, economic, and political means of influence, which significantly complicates its identification, counteraction, and neutralization. T. Solmaz (2022) identifies several primary interpretations of this term. These interpretations include the combination of conventional weapons, irregular tactics, terrorism, and criminal activity within a unified battlespace; the coordinated utilization of regular and irregular forces under unified command; the application of various military and non-military means to threaten an adversary; actions below the threshold of open warfare that include any combination of violent and non-violent means; and the achievement of political objectives through non-violent subversive measures. Since the term's popularization by F. Hoffman (2007), the concept of "hybrid warfare" has undergone significant modifications and expansions. The absence of a unified definition complicates understanding and effective response to such threats by Western countries. In their official documents, NATO and the EU characterize "hybrid warfare" as a method of achieving political objectives through a mixture of kinetic and non-kinetic means while remaining below the threshold of traditional warfare

In general, the concept of "hybrid warfare" is vast and ambiguous, which complicates its practical application. This ambiguity creates confusion between states of war and peace, consequently hampering strategic planning efforts. Many surveyed NATO officials contend that "hybrid warfare" does not represent a novel phenomenon, but rather serves as a contemporary designation for traditional warfare methods that combine regular and irregular elements (Caliskan & Liégeois, 2020).

Following the Russian Federation's annexation of the Autonomous Republic of Crimea in 2014, NATO adopted the term "hybrid warfare" to designate the new form of armed conflict that emerged from Russia's actions in Ukraine. This linguistic choice represents a pivotal stage in the evolution of the "hybrid warfare" concept. First, the use and dissemination of this term in Western military and strategic discussions increased significantly. Second, considering that Russian activities in Ukraine did not fully align with existing theoretical models of hybrid warfare, the concept underwent further conceptual expansion. Overall, the Russian Federation pursued its political objectives through a combination of non-kinetic means – including cyber attacks, information-psychological operations, propaganda, disinformation, economic pressure, and diplomatic influence – alongside military instruments, particularly covert operations and intensified proxy structure activities.

Hybrid warfare in contemporary international law doctrine is defined as a collection of strategies, tactics, and methods that combine military, political, economic, informational, and cyber components, aimed at achieving political and strategic objectives without a formal declaration of war. The principal characteristic of hybrid warfare lies in its utilization of diverse means and methods, which may be unconventional and not necessarily military in nature (Glukh, Honcharenko, 2024: 203).

Weissmann, M., Nilsson, N., Palmertz, B., and Thunholm, P. examine hybrid warfare as a military strategy that combines conventional warfare, so-called "irregular warfare", and cyberattacks with other methods of influence, such as fake news, diplomacy, and foreign policy intervention (Weissmann et al., 2021).

In contemporary reality, hybrid warfare represents a complex strategic approach that involves the integration of both state and non-state actors into a broad, multi-component, adaptive, and often highly integrated combination of traditional and non-traditional means of warfare. One of the main goals of employing a hybrid strategy is to achieve political or military results without initiating open armed conflict while keeping the tools employed below the threshold defined by international law as an "armed attack".

Such strategy aims to undermine, destabilize, or weaken the political system, social cohesion, and sovereignty of the target state through a combination of violence, control, destructive activities, information-psychological manipulations, and the spread of disinformation. Hybrid warfare provides states with tools to influence the sovereign processes of other countries or the ability to disrupt them without the need to report to domestic political institutions or the national electorate (Bachmann et al., 2023).

Contemporary hybrid warfare transcends traditional military operations, encompassing psychological and informational dimensions that significantly influence conflict trajectories. Hybrid warfare involves the utilization of non-military instruments, including information operations, cyber attacks, and influence through proxy groups, to achieve strategic objectives without direct military intervention (Matveev et al., 2021). Particular emphasis is placed on shaping public opinion and the psychological condition of populations in target countries through information campaigns and disinformation, as well as engaging sympathetic third-party groups or organizations to exert influence or destabilize situations within target countries. A. Manolea (2021) highlights that the concept of "hybrid warfare" remains highly contested despite its popularity. Five major interpretations of hybrid warfare are identified, ranging from the fusion of conventional and irregular tactics in the same battlespace to achieving political goals through non-violent subversive activities.

Hybrid warfare involves the deployment of both state and non-state actors utilizing diverse military and militarized strategies, which significantly complicates adherence to and assessment of international humanitarian law, particularly regarding the principle of state responsibility. In hybrid warfare, tactical and strategic goals often take precedence over civilian protection. This prioritization results in substantial humanitarian and medical consequences, encompassing direct civilian casualties, destruction of medical infrastructure, and long-term population health implications (Khorram-Manesh and Burkle, 2022).

The strategic orientation of hybrid warfare centers on the destabilization and paralysis of critical societal infrastructure components, including legal institutions, healthcare systems, food security mechanisms, transportation networks, economic structures, and other essential domains that constitute state resilience. Its fundamental objective involves civilian population influence as a means of realizing the aggressor's political aims. A distinctive characteristic of hybrid warfare involves the systematic implementation of disinformation, manipulation, and deception across political, social, and military spheres. Specifically, the proliferation of fabricated news content and propaganda narratives impedes international institutions' capacity to document international humanitarian law violations and Geneva Conventions infractions. Furthermore, the systematic application of psychological pressure methodologies, including intimidation and coercive threats, aims to intensify fear and disorder among occupied territories' populations, consequently undermining collective morale, exacerbating societal hostilities, and diminishing civil resistance capabilities (Khorram-Manesh et al., 2023).

Hybrid warfare represents an emergent dimension in contemporary conflict paradigms, characterized by the integration of diverse military and non-military instruments for strategic objective attainment. The fundamental essence of this strategic approach resides in the deployment of a comprehensive spectrum of instruments, encompassing information warfare, economic coercion, cyber operations, diplomatic leverage, terrorism, and additional non-conventional aggression modalities. Social media platforms and mass communication channels constitute critical elements within this destabilization framework (Savliuk, 2024).

Characteristic components of hybrid warfare encompass multifaceted methodologies designed to catalyze and intensify internal conflict dynamics within target states. These methodologies include the generation of societal fissures through systematic propaganda deployment, which subsequently evolves into comprehensive information warfare operations; the initiation and exacerbation of economic vulnerabilities through confrontational economic measures, manifesting as trade warfare and systematic disruption of the target state's relationships with adjacent nations and international partners. Supplementary instruments include material support for separatist and terrorist entities, encompassing financial backing and armament provision, potentially extending to state-sponsored terrorism; the establishment of quasi-governmental structures as components within hybrid state-formation initiatives; and the facilitation of irregular (pseudo-military) armed formation development and their subsequent material-technical resource provisioning.

Publications by Ukrainian researchers (Buriachenko, 2024; Derevyanko, 2023; Savliuk, 2024) demonstrate a consistent analytical position wherein multidimensional influence instruments constitute the definitive components of hybrid warfare, deployed simultaneously to achieve strategic advantage over adversaries. These components encompass military, political, economic, informational, ideological, psychological, technological, and energy-related influence mechanisms.

The Russian Federation implements a comprehensive hybrid strategy against Ukraine that permeates various societal domains, including the customs system. A significant segment of Ukraine's population becomes involved in this process, both at conscious and unconscious levels. Russian strategic operations actively employ propaganda and disinformation methodologies to undermine confidence in Ukrainian state institutions, particularly the customs service. This manifestation is evident through the systematic dissemination of fabricated information designed to discredit customs authorities and their personnel.

In the contemporary information era, national development as a systemic formation is fundamentally determined by the level of information culture attained: nations that establish information leadership typically influence global economic policy development through the imposition of their information products and services upon information-peripheral entities (Lomachinska & Bondar, 2019: 84). Within armed conflict contexts, the fundamental human right to information access acquires particular significance, functioning simultaneously as a communication facilitation mechanism and as a potential manipulative influence instrument. Under such circumstances, the implementation of this right must prioritize guaranteed access to reliable, verified information; facilitation of civil society mobilization for resistance against aggression; consolidation of international community support for Ukraine; and the strategic utilization of information resources as countermeasures within information warfare paradigms.

To address these imperatives in practical terms, Ukraine must adopt a coherent, policy-driven response to information warfare. Ukraine's response to information warfare requires translating media literacy principles into actionable strategies through state-coordinated education. Integrating critical media analysis into school and university curricula is essential, focusing on skills like identifying manipulation, cross-checking sources, and recognizing propaganda – fundamental competencies in conflict zones. Beyond formal education, partnerships between government, civil society, and independent media can extend impact through targeted awareness campaigns, accessible digital workshops, and centralized fact-checking resources. These collaborations not only help citizens navigate misinformation but encourage active participation in countering harmful narratives. Strategic use of digital platforms for real-time information verification addresses transparency gaps and helps rebuild institutional trust undermined by disinformation. By combining government resources with grassroots expertise, Ukraine can develop a population capable of withstanding information threats while maintaining social cohesion during hybrid warfare. These approaches, while specific to Ukraine's context, offer broader insights for information integrity during conflict situations.

Significant attention must be directed toward counteracting the Russian Federation's information expansion, which employs information weapons to undermine Ukraine's information sovereignty. Within this framework, the development of strategic state information and communication policy acquires paramount importance, oriented toward prevention, counteraction, and neutralization of destructive information-psychological influence on public consciousness across national, regional, and local levels (Radchenko, Chmyr, 2022).

Digital media literacy represents a foundational element in promoting healthier social media engagement practices and functions as a catalyst in combating misinformation proliferation. The implementation of governmental digital and media education development initiatives and the cultivation of individual critical assessment capabilities constitutes an effective countermeasure against contemporary information challenges (Lomachinska & Lomachynskyi, 2022: 72).

O. Buriachenko (2024) emphasizes that hybrid warfare has emerged as a central instrument of global policy, necessitating novel strategic approaches to national and international security provision. Specifically, through customs tariff manipulation, trade blockades, and additional economic measures, the Russian Federation attempts to destabilize Ukraine's economic foundation and compromise its foreign economic relationships.

Within the hybrid warfare framework, the Russian Federation implements numerous economic strategies designed to weaken Ukraine's customs system and destabilize its overall economic structure. These actions aim to reduce state budget revenues, undermine institutional credibility, and establish conditions for political leverage. Among primary economic influence strategies, the aggressor state employs trade restrictions and embargoes, systematically prohibiting Ukrainian goods importation, particularly agricultural and food products; these measures generate substantial economic losses for Ukrainian exporters and diminish budget revenues through reduced customs payments. Additionally, natural gas supply manipulation, establishment of unfavorable contract conditions, and strategic pricing policies function as instruments of influence on Ukraine's economy. Through transit agreement violations, Russia restricts Ukrainian goods transit to third countries via its territory, resulting in logistical chain disruptions and customs revenue reduction (Ishchuk, 2024). Information campaigns against customs authorities constitute another prevalent hybrid influence strategy, as disinformation dissemination regarding Ukrainian customs corruption and inefficiency undermines institutional credibility and contributes to internal destabilization.

Within the context of hybrid threats, the digitalization of Ukraine's customs system represents a critically important component of comprehensive public administration and security reform, holding strategic significance for both internal stability and European integration advancement.

The Ukrainian Parliament, government, and specialized executive authorities have enacted a substantial body of normative-legal documents that not only simplify customs control procedures and goods and transport vehicle clearance processes but also provide specific customs payment privileges for importers. Wartime challenges have measurably impacted State Customs Service operational indicators. Ukrainian customs operations require synchronization with European Union member states' customs administrations, which would facilitate expedited cross-border goods movement and optimally support international trade activities (Merezhko et al., 2022).

The reform of the State Customs Service of Ukraine involves a far-reaching digital transformation aimed at modernizing core services and improving the efficiency of customs procedures. It focuses on six interrelated areas: the development of a Single Window system, improvements in customs control and clearance, enhanced public reporting and data analytics, the implementation of Smart Customs Checkpoints, strengthened cybersecurity measures, and the harmonization of Ukrainian customs legislation with that of the European Union. These efforts are intended to promote digital integration and more effective cooperation between customs authorities, international partners, and foreign trade operators. This approach reflects global trends in facilitating international trade, enhancing public sector transparency, combating smuggling, and ensuring the efficient collection of customs revenues.

Amid Russia's ongoing hybrid aggression, the digitalization of customs functions plays a critical role in safeguarding critical infrastructure, protecting information systems, and securing logistics channels. The use of advanced risk management systems enables authorities to promptly identify irregularities in customs procedures and to disrupt both smuggling operations and the financial support of subversive activities (State Customs Service of Ukraine).

The e-Customs program is aimed at transforming traditional paper-based procedures into digital operational processes. This transition supports the creation of a more efficient, transparent, and technologically advanced customs environment that meets the demands of the global economy. Within this framework, customs authorities focus on developing and implementing digital solutions and services that streamline the work of foreign economic operators, border control agencies, and customs officials (Matsedonska et al., 2021).

Since the onset of Russia's full-scale invasion, the State Customs Service of Ukraine has become one of the first institutions whose operations underwent significant changes in order to ensure the rapid importation and customs clearance of goods essential under martial law conditions.

A key aspect of the reform structure is the "Public Reporting and Analytics" component, which involves the launch and maintenance of open data services. This component aims to enhance the transparency of the customs system and expand the functional capabilities of its information infrastructure. The use of information and communication technologies significantly reduces the time required for customs procedures, lowers the administrative burden on businesses, and decreases the risks of corruption. For example, the electronic decision-making system for Binding Tariff Information (BTI) creates predictability in the classification of goods and reduces the potential for abuse. (State Customs Service of Ukraine, 2023).

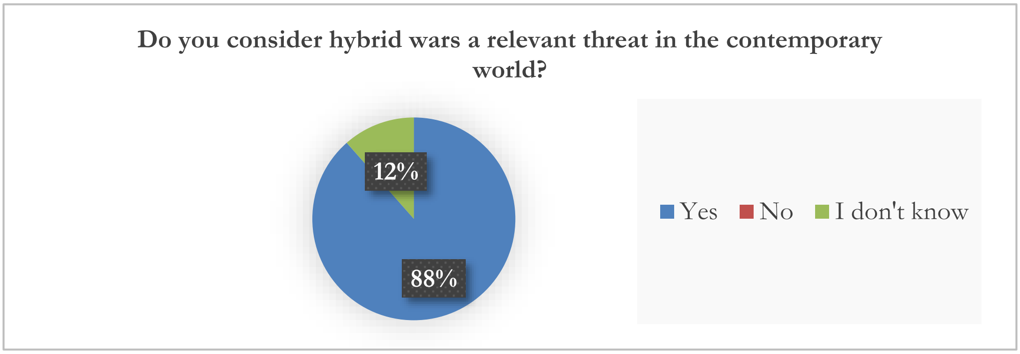
The further development of digitalization is based on the active use of innovative information and communication technologies, which enhance operational efficiency, ensure rapid data flow, automate control procedures, and reduce human intervention in decision-making. The application of such technologies contributes to the improvement of business processes in international trade, lowers transaction costs, and strengthens the competitiveness of the national economy. The adoption of digital solutions in these areas not only enhances the effectiveness of customs administration but also strengthens integration with the European customs system, ensuring compliance with EU standards and the principles of open government.

In 2025, the State Customs Service of Ukraine (SCSU) continues its active digital transformation aimed at improving the effectiveness of customs control and countering hybrid threats, particularly those from the Russian Federation. These measures are designed to strengthen national security and facilitate integration into the European customs space. One of the key projects is the development of an automated system for handling customs authority decisions (CDS.UA), based on the European prototype Customs Decision System (CDS). This system allows foreign economic operators to submit applications for customs decisions in electronic format, ensuring transparency and reducing corruption risks. CDS.UA integrates with other SCSU information systems, including the Single Window module and the automated risk management system, enhancing the efficiency of customs control and supporting the rapid detection of violations. In the Public Reporting and Analytics area, SCSU is implementing open data services, such as the online customs payment calculator and the tool for determining the Ukrainian Classification of Commodities in Foreign Trade code. These tools contribute to the automation of internal reporting and the implementation of analytical tools to detect anomalies in customs operations, which is crucial in the context of countering hybrid threats.

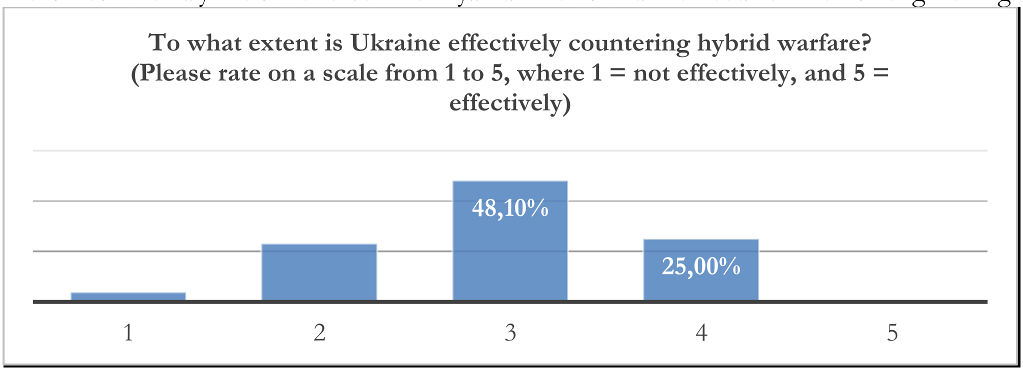
Digitalization of customs policy in Ukraine is an important stage in the modernization of public administration, but this process faces several significant challenges that need to be addressed. Among the key issues are insufficient levels of digital literacy, cybersecurity concerns, as well as institutional and legal barriers that could slow the effective implementation of digital technologies in the customs sector. However, to achieve full digital transformation, several challenges must be overcome, particularly enhancing digital literacy and ensuring robust cybersecurity. An important step is also adapting Ukrainian customs procedures to international standards and implementing innovative technologies (Mygal, 2025).

In this context, the customs system of Ukraine serves not only as a fiscal tool but also as a key element of national security, economic resilience, and legal integration into the European space. Given the hybrid nature of the threats, the digitalization of the customs infrastructure is becoming particularly urgent. The introduction of digital technologies in customs administration meets not only the needs of rapid response but also the principles of sustainable development, particularly through: enhancing institutional transparency and accountability; effective resource management and minimizing corruption risks; ensuring continuity and reliability of public administration even in the face of crises; and fostering the creation of a favorable environment for international trade and economic growth.

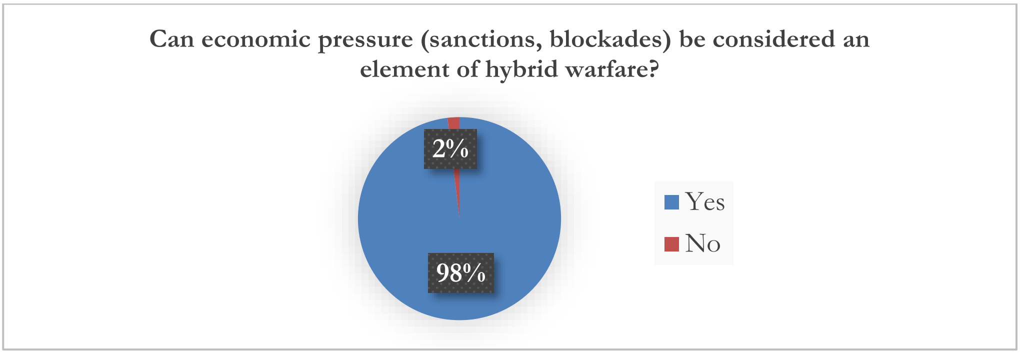
Based on a survey conducted among 215 students from the State Tax University (Irpin, Ukraine), Borys Grinchenko Kyiv Metropolitan University (Kyiv), the National University of Construction and Architecture (Kyiv), and the Hetman Petro Sahaydachnyi National Army Academy (Lviv, Ukraine), 88% of respondents noted the relevance of the threat of hybrid wars.



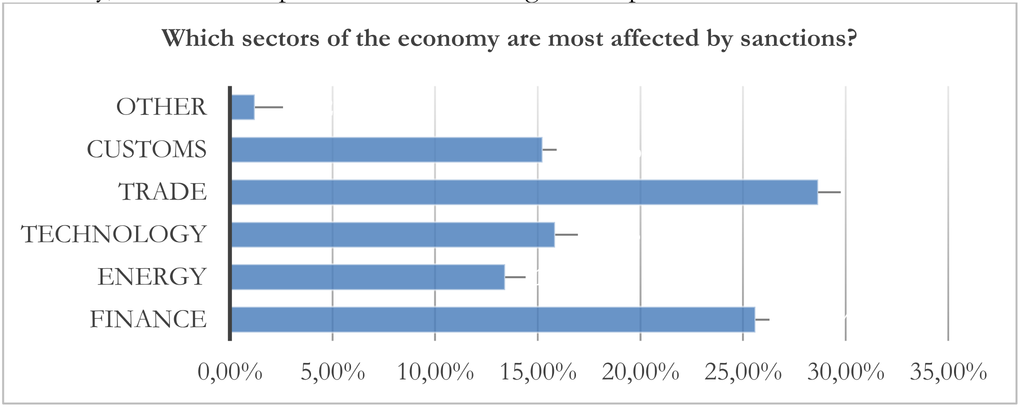
The majority of respondents assessed the level of Ukraine's protection against hybrid threats as moderate, indicating an adequate awareness within society of the measures taken by the state to counter hybrid threats and the need for their strengthening:



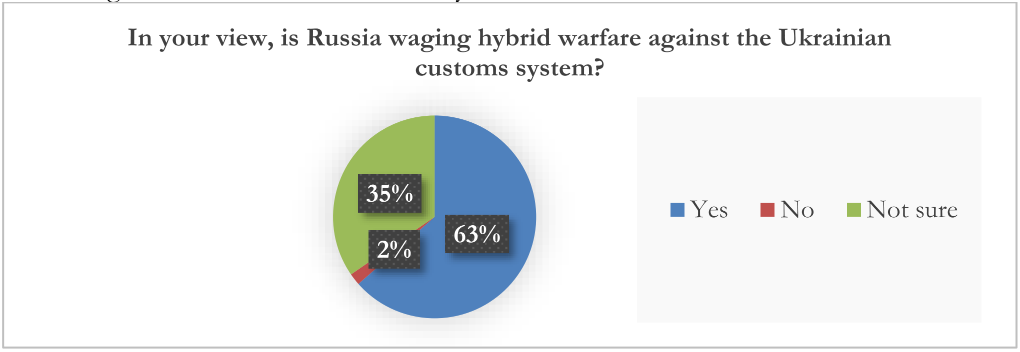
Economic pressure as an element of hybrid warfare was identified by 98% of respondents:



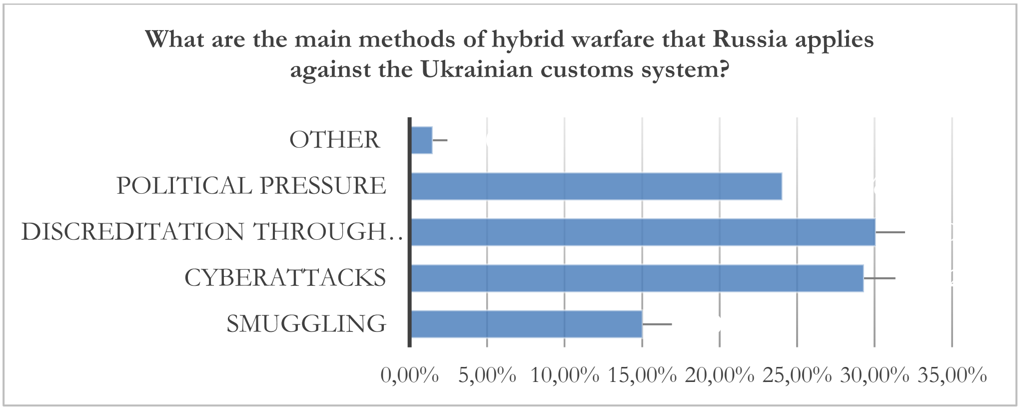
Analyzing the economic consequences of hybrid warfare in various sectors of the economy, 15.24% of respondents noted its negative impact on customs:



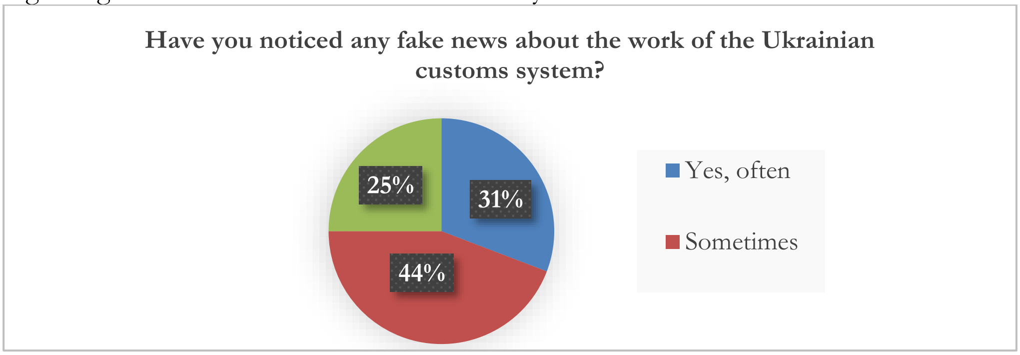
The vast majority, 63% of respondents, believe that Russia is waging hybrid warfare against the Ukrainian customs system:



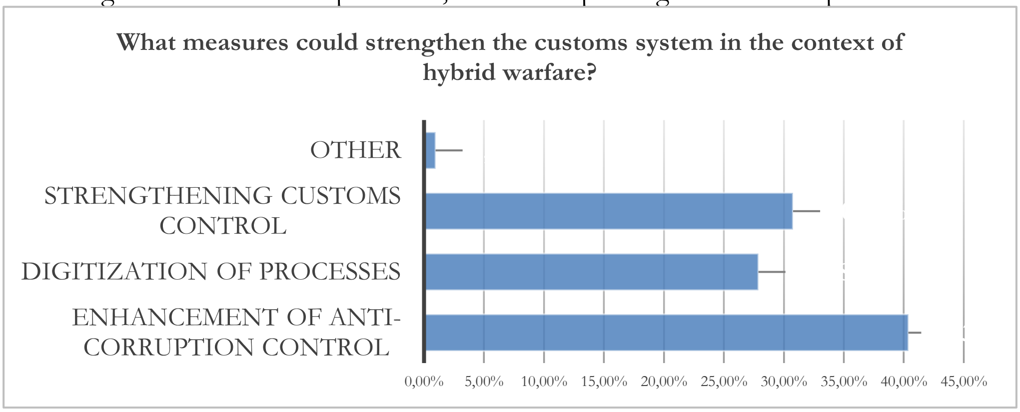
Among the main methods used by Russia against Ukrainian customs, survey participants identified discreditation through propaganda, cyberattacks, and political pressure:



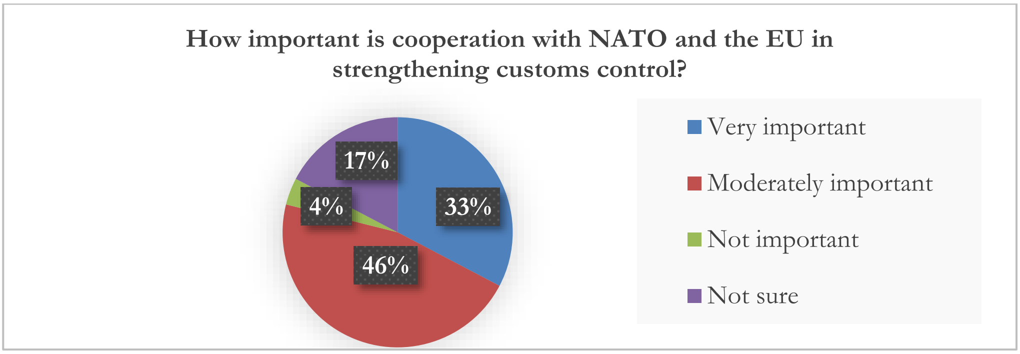
Specifically, 75% of respondents noticed fake news in the information space regarding the work of the Ukrainian customs system:



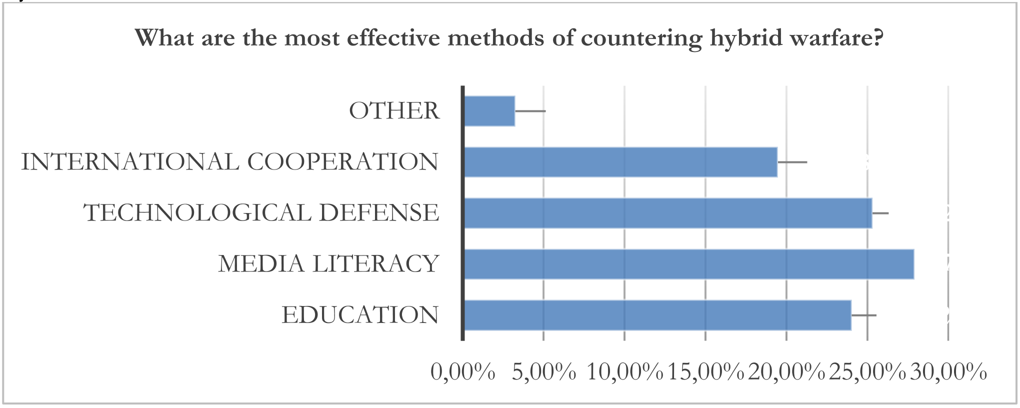
One of the most effective measures to counter hybrid threats to customs, according to the respondents, is improving anti-corruption control:



The importance of strengthening cooperation with NATO and the EU is emphasized by 79% of respondents:



Among the most effective methods for countering hybrid warfare, respondents identified media literacy, technological defense, and education; additionally, one-fifth of the participants highlighted the importance of international cooperation in countering hybrid threats.



Thus, the survey results confirm the key scientific propositions reflected in the study.

We support the position of Ukrainian researchers (Derevianko, 2024), who argue that, in the context of countering hybrid warfare, conducting large-scale analytical studies on the assessment and improvement of national information policy is both appropriate and promising. This is aimed at preventing and neutralizing threats to national security (Kryvyzyuk et al., 2021). Particular attention should be given to involving civil society institutions, expert communities, and critically analyzing and adapting international experience in the field of information security.

Counteracting manifestations of hybrid warfare requires Ukraine to implement a set of systemic measures aimed at ensuring national security in the information sphere, particularly within the activities of customs structures. Key response areas include: the protection of information and communication infrastructure, computer systems, information networks, and databases; the establishment of specialized units and services responsible for safeguarding information resources from unauthorized access and cyber threats, such as hacker attacks, among others. Strengthening customs infrastructure through digitization contributes to increased budget revenues, protection of the domestic market, and prevention of losses from the illegal export of strategically important products. This, in turn, ensures the financial stability of the state in the context of military conflict.

5. Limitation on the Study

A key limitation of our study lies in its reliance on student perceptions to evaluate hybrid threats and customs vulnerabilities. While their academic perspectives offer valuable insight, they do not fully capture the operational realities of hybrid warfare. Including views from customs officials, security experts, and policymakers would provide a more comprehensive and representative understanding. Future research should adopt a multi-stakeholder approach to strengthen the practical applicability of findings.

6. Conclusions

According to modern international law doctrine, hybrid warfare is defined as a comprehensive form of conflict that combines military, political, economic, informational, and cybernetic instruments of influence to achieve strategic and political objectives without the formal declaration of war. This phenomenon exerts a destructive impact on political stability, social cohesion, and state sovereignty through a combination of violence, informational-psychological manipulation, disinformation, economic pressure, and the undermining of state institutions.

In the context of Ukraine's current security situation, hybrid warfare extends beyond traditional armed conflict, encompassing new domains – particularly psychological, informational, and economic spheres. A key area of focus is the manipulation of public opinion through the systematic dissemination of fake news, discrediting institutions, generating panic, and eroding trust in state power. Such actions complicate the efforts of international organizations, particularly with regard to documenting violations of international humanitarian law, and create obstacles to the sustainable functioning of essential state institutions.

Economic instruments of hybrid influence, especially those aimed at destabilizing Ukraine's customs system, present a specific threat. Targeted informational attacks on customs authorities, including the spread of claims about systemic corruption and inefficiency, are designed to undermine the legitimacy of state institutions and erode public support for reforms. Combined with direct economic pressures, such as the blockade of trade routes or the destruction of logistical infrastructure, these actions create barriers to sustainable socio-economic development.

In response, the digital transformation of the customs system represents a strategic countermeasure to multifaceted hybrid threats, bolstering institutional resilience, increasing social trust, and enhancing Ukraine's position in global economic networks. Ukraine's participation in the European Union's digital customs initiatives is not only an element of fulfilling foreign policy obligations but also a strategic factor in achieving sustainable development goals, contributing to the establishment of resilient institutional foundations for effective post-conflict recovery. Future research should assess the long-term implications of these reforms, including their influence on foreign investment confidence, trade volume, and regional economic cooperation amid ongoing hybrid threats. Empirical analysis in these areas would clarify the structural role of digital customs in Ukraine's post-war economic integration.

References

Bachmann, S. D., Putter, D., Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. Global Policy, 14(5), 858–869. https://doi.org/10.1111/1758-5899.13257

Bilovodska, O., Khurdei, V. (2024). Strategy of customs business services based on marketing management. Customs Scientific Journal, 1, 19–27. https://doi.org/10.32782/2308-6971/2024.1.2

Bluszcz, J., Valente, M. (2022). The economic costs of hybrid wars: The case of Ukraine. Defence and Peace Economics, 33(1), 1–25. https://doi.org/10.1080/10242694.2020.1791616

Buriachenko, O. (2024). Hybrid warfare as a new form of global confrontation. Scientific Works of the Interregional Academy of Personnel Management. Political Science and Public Administration, 2(74), 24–31. https://doi.org/10.32689/2523-4625-2024-2(74)-3

Caliskan, M., Liégeois, M. (2020). The concept of 'hybrid warfare' undermines NATO's strategic thinking: Insights from interviews with NATO officials. Small Wars & Insurgencies, 32(2), 295–319. https://doi.org/10.1080/09592318.2020.1860374

Derevianko, S. (2024). Hybrid warfare: information and security dimension. Bulletin of the Precarpathian University. Series: Political Science, 18, 101–113. https://doi.org/10.32782/2312-1815/2024-18-11

Derevyanko, I. (2023). Hybrid warfare as a type of asymmetric action. International Relations: Theoretical and Practical Aspects, 11, 6–16. https://doi.org/10.31866/2616-745X.11.2023.278396

Eberle, J., Daniel, J. (2022). Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. Political Geography, 92, 102502. https://doi.org/10.1016/j.polgeo.2021.102502

Glukh, M., Honcharenko, M. (2024). The essential understanding and nature of the concept of "hybrid warfare" in the modern doctrine of international law. Irpin Law Journal: Scientific Journal, 1(14), 197–205. https://doi.org/10.33244/2617-4154-1(14)-2024-197-205

Guidelines for Customs Policy in Ukraine. (2020). The American Chamber of Commerce in Ukraine. Retrieved May 16, 2025, from https://chamber.ua/wp-content/uploads/2020/01/guidelines_for_customs_policy_in_ukraine_en.pdf

Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies.

Ishchuk, M. (2024). Customs payment evasion and the shadow economy: navigating challenges in Ukraine's war context. Pryazovskyi Economic Herald, 4(40), 56–62. https://doi.org/10.32782/2522-4263/2024-4-11

Khorram-Manesh, A., Burkle, F. M., Jr. (2022). Civilian population victimization: A systematic review comparing humanitarian and health outcomes in conventional and hybrid warfare. Disaster Medicine and Public Health Preparedness, 17, e192. https://doi.org/10.1017/dmp.2022.96

Khorram-Manesh, A., Goniewicz, K., Burkle, F. M., Jr. (2023). Social and healthcare impacts of the Russian-led hybrid war in Ukraine – A conflict with unique global consequences. Disaster Medicine and Public Health Preparedness. https://doi.org/10.1017/dmp.2023.91

Kryvyzyuk, L., Levyk, B., Khrypko, S., Ishchuk, A. (2021). The Phenomenon of National Security within Postmodern Cultures: Interests, Values, Mentality. Postmodern Openings, 12(3), 77–95. https://doi.org/10.18662/po/12.3/328

Lomachinska, I., Bondar, T. (2019). The ideological essence of the phenomenon of information culture in the context of modern globalization challenges. Bulletin of the National Academy of Managerial Staff of Culture and Arts, (1), 61–85. https://doi.org/10.32461/2226-3209.1.2019.166545

Lomachinska, I., Lomachynskyi, B. (2022). The role of media culture in modern information wars. SKHID, 3(3), 66–73. https://doi.org/10.21847/1728-9343.2022.3(3).268297

Manolea, A. (2021). The transpersonal war – constituent of the hybrid war. Land Forces Academy Review, 26(4), 372–376. https://doi.org/10.2478/raft-2021-0048

Matsedonska, N., Kovalenko, V., Shtefan, L. (2021). Modernization of customs activities using information technologies. Economy and Society, (27). https://doi.org/10.32782/2524-0072/2021-27-16

Matveev, V., Nykytchenko, O., Stefanova, N., Khrypko, S., Ishchuk, A., Pasko, K. (2021). Cybercrime as a Discourse of Interpretations: the Semantics of Speech Silence vs Psychological Motivation for

Actual Trouble. International Journal of Computer Science and Network Security, 21(8), 203–211. https://doi.org/10.22937/IJCSNS.2021.21.8.27

Merezhko, N., Karavayev, T., Kaluha, N. (2022). Customs policy of Ukraine during the armed aggression of the Russian Federation. International Trade, (6), 4–16. https://doi.org/10.31617/3.2022(125)01

Mumford, A. (Ed.). (2018). Hybrid warfare: Security and asymmetric conflict in international relations. Bloomsbury Publishing. Retrieved April 15, 2025, from https://library.oapen.org/bitstream/handle/20.500.12657/58862/9781786736550.pdf?sequence=1&isAllowed=y

Mygal, M. (2025). The road to the EU: The role of digitalisation in reforming the State Customs Service. Institute for Analysis and Advocacy. Retrieved April 15, 2025, from https://iaa.org.ua/articles/road-to-the-eu-the-role-of-digitalisation-in-reforming-the-state-customs-service/

Mykuliak, O., Stefanyshyn, R. (2019). Introduction of information technologies in the customs practice of Ukraine. World of Finance, 4(61), 53–66. https://doi.org/10.35774/sf2019.04.053

Radchenko, O., Chmyr, Ya. (2022). Hybrid war as a key threat to the national sovereignty of Ukraine. Taurida Scientific Herald, (3), 100–108. https://doi.org/10.32851/tnv-pub.2021.3.14

Savliuk, M. (2024). Hybrid warfare in Ukraine: contemporary approaches. Newsletter of the Precarpathian University. Series: Politology, 17, 187–197. https://doi.org/10.32782/2312-1815/2024-17-23

Solmaz, T. (2022). "Hybrid warfare" is one term with many meanings. Conservative News Daily. Retrieved April 15, 2025, from https://www.conservativenewsdaily.net/breaking-news/hybrid-warfare-is-one-term-with-many-meanings/

State Customs Service of Ukraine. (2023). EU integration IT implementation of the State Customs Service – electronic system for binding information decisions. Retrieved April 15, 2025, from https://customs.gov.ua/news/it-transformatsiia-62/post/ievrointegratsiine-it-vprovadzhennia-derzhmitsluzhbi-elektronna-sistema-roboti-z-rishenniami-shchodo-zobov-iazuiuchoyi-informatsiyi-1527

State Customs Service of Ukraine. Customs IT transformation: Testing of the updated risk management system ASUR 2.0 has started. Retrieved April 15, 2025, from https://customs.gov.ua/en/news/novini-20/post/it-transformatsiia-mitnitsi-rozpochato-viprobuvannia-onovlenoyi-sistemi-upravlinnia-rizikami-asur-2-0-439

Steingartner, W., Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. Acta Polytechnica Hungarica, 18(3), 25–45. https://doi.org/10.5040/9781788317795

Weissmann, M., Nilsson, N., Palmertz, B., Thunholm, P. (2021). Hybrid warfare: Security and asymmetric conflict in international relations. I.B. Tauris.